



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Patent and Trademark Office**

Address: COMMISSIONER OF PATENTS AND TRADEMARKS  
Washington, D.C. 20231

*BCJ*

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
-----------------	-------------	----------------------	---------------------

09/328,726	10/26/98	COLLINS	T 2026-25 (PT-T)
------------	----------	---------	------------------

┌

WM31/0814

└

EXAMINER
----------

LEAH SHERRY  
OPPENHEIMER, WOLFF & DONNELLY, LLP  
1400 PAGE MILL ROAD  
PALO ALTO CA 94304

LEANING, J

ART UNIT	PAPER NUMBER
----------	--------------

2131

*21*

DATE MAILED:

08/14/01

**Please find below and/or attached an Office communication concerning this application or proceeding.**

**Commissioner of Patents and Trademarks**

## Office Action Summary

Application No.

09/328,726

Applicant(s)

COLLINS ET AL.

Examiner

Jeffrey Scott Leaning

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 18 June 2001.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 14-92 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 14-92 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

### Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892) 4) ☐ Interview Summary (PTO-413) Paper No(s) \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948) 5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_ 6) ☐ Other: \_\_\_\_\_

Art Unit: 2131

### DETAILED ACTION

1. Claims 14-92 are pending in the present application. Claims 14-92 stand rejected.
2. Due to the notation-intensive nature of the application, the examiner will state the conventions that he will use. Underscore marks will denote subscripts, so "a sub" will be denoted by "a<sub>b</sub>". Carets will denote superscripts, so "a to the b" will be denoted by "a<sup>b</sup>".

### *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 14-46 are rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. See the enumerated items below.
5. Claims 14-46 are also rejected under 35 U.S.C. 112, first paragraph, as containing subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. *The applicant is required to either cancel the claims as referring to new matter or address their support.*

Art Unit: 2131

a. Claims 14, 15, 16, 22, 27, 32, 37, and 42 as amended, include the provision of being "backwards compatible with preexisting public key transformation schemes".

i. The applicant has provided no disclosure as to how the claimed invention is backwards compatible with anything. The applicant has pointed to lines 12-16 of page 7 of the disclosure which states in part, "other advantages of the invention include its employment for decryption without the need to revise the RSA public encryption transformation scheme currently in use on thousands of large and small computers." This single conclusionary sentence is relied upon by the applicant to support the contention that the claimed invention would work harmoniously with the public key transformations currently in use.

ii. The alleged backwards compatibility of one cryptosystem with another is a non-trivial problem to be solved. There are many obstacles to overcome, not the least of which is as follows. The applicant's cryptosystem is directed to a multi-prime (three or more) RSA type system. A message encrypted using the applicant's system would require decryption on a system using at least three primes. There is no way that a standard two-prime RSA system could conceivably decrypt a message which was encrypted using three or more primes. *The applicant's system is not backwards compatible with existing RSA systems because existing two-prime systems could not decrypt messages which were encrypted using the applicant's three-or-more prime system.*

b. Claims 14 and 15 recite that the "step of decoding is accelerated". This term is not disclosed by the applicant, nor is it enabled by the specification. The examiner requests that the

Art Unit: 2131

applicant point out where in the specification the term "step of decoding is accelerated" appears, or, barring that, where in the specification support appears for this expedient.

c. Claims not specifically addressed are rejected by virtue of their dependence on rejected claims.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 14 and 15 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. These claims recite that the "step of decoding is accelerated". The scope of this term is unclear for the following reasons. The term "accelerated" is relative. That is, something is accelerated only in relation to a fixed velocity. "Accelerated" means having increasing velocity. It is unclear how a decoding can have an increasing velocity. The time interval over which it is increasing is of uncertain scope. For example, this phrase may be interpreted as meaning the decoding requires less time to run with each consecutive execution. This action is not supported by the specification to the extent required to render it of definite scope. For the purposes of this action, the examiner interprets this term to mean that the algorithm is somehow efficient or fast.

Art Unit: 2131

***Claim Rejections - 35 USC § 102***

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 14-66 rejected under 35 U.S.C. 102(b) as being anticipated by Rivest *et al* (US 4,405,829).

a. Claim 14 is directed to an RSA type system including encryption and decryption. Rivest *et al* disclose this system, see the summary of the invention starting on line 12 of column 4. Additionally, the applicant's invention is particularly directed to the following two features: (1) using more than two primes in the modulus, and (2) using the Chinese Remainder Theorem to speed up decryption. Rivest *et al* also discloses both of those features, see column 13 lines 29-34. The particular equations specified in claim 14 lines 11-24 and 30-32, and in the corresponding parts of the other claims, are inherent in using the Chinese Remainder Theorem for decoding as taught by Rivest *et al*.

b. Claim 15 is similar to claim 14 except the message is decrypted using the corresponding formulae and steps. See the above.

c. Claim 16 is a system embodiment which includes the encoding of claim 14 and the decoding of claim 15 and is rejected on analogous grounds as being obvious as such.

Art Unit: 2131

d. Claims 17-21 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

e. Claims 22-26 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.

f. Claims 27-31 are method claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

g. Claims 32-36 are system claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.

h. Claims 37-41 are method claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 15.

i. Claims 42-46 are system claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 16.

j. Rivest *et al* also disclose that their invention can digitally sign and verify digital signatures, see column 4 lines 1-6, and the summary of using their invention in that capacity starting at column 5 line 18.

i. Claims 47-51 are method claims for signing a message and are rejected on grounds analogous to those used to reject claims 14 and 15 and further in light of paragraph j above.

Art Unit: 2131

ii. Claims 52-56 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

iii. Claims 57-61 are procedure claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

iv. Claims 62-66 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of paragraph j above.

***Claim Rejections - 35 USC § 103***

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

11. Claims 67-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest *et al* as applied above, and further in view of Menezes *et al*. Claims 67-92 are dependent claims which are directed to two features. The examiner addresses them here.

a. Claims 67 *et al* are directed to processing the sub-tasks by way of a plurality of exponentiation units operating substantially independently. Menezes *et al* discloses simultaneous



Art Unit: 2131

multiple exponentiation, see Note 14.87(iii) on page 617. It would be obvious to one of ordinary skill in the art to use this method in the invention of Rivest *et al* because of Menezes *et al*'s suggestion that efficient exponentiation is essential to employing the RSA algorithm, see the first two paragraphs of Section 14.6 Exponentiation on page 613.

b. Claims 68 *et al* are directed to insuring that each of the random primes has the same number of bits. Menezes *et al* discloses that each of the primes used should be "roughly the same size". It would be obvious to one of ordinary skill in the art to ensure that the number of bits for each of the primes is the same size in the invention of Rivest *et al* because of Menezes *et al*'s suggestion that they should be roughly the same size. Note that "roughly the same size" discloses a range which includes identity.

12. Claims 14-92 rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes *et al* in view of Quisquater *et al*.

a. Claim 14 is directed to a method for establishing cryptographic communications. Menezes *et al* teach of a computation method for processing secret information, see section 8.2 (pp. 285-291).

i. Both Section 8.2 of Menezes *et al* and the applicants use RSA-type cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Section 8.2, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants there are possibly more than two prime numbers in the modulus and

Art Unit: 2131

they are called  $p_1, p_2, \dots, p_n$ . Hence,  $p$  corresponds to  $p_1$ , and  $q$  corresponds to  $p_2$ . This is merely notation, and the examiner point it out for the sake of clarity. The essential features are identical.

ii. Menezes *et al* teach of encoding a plaintext word  $M$  to a ciphertext word  $C$ , see Algorithm 8.3. Menezes *et al* disclose that  $M$  is of a certain size, less than a fixed size, see Message Blocking on page 285. It is inherent that the message block size for RSA (the method of section 8.2) is  $n-1$  where  $n$  is the product of prime integers.

iii. Menezes *et al* teach of transforming ciphertext  $C$  to message  $M$ , see Algorithm 8.3. Note that a corresponding decryption is also disclosed.

iv. The number ' $e$ ' is selected as being relatively prime to the described lcm (least common multiple), see Algorithm 8.1 and Note 8.5.

v. Section 8.2 of Menezes *et al* lacks a teaching that there can be more than two primes in the modulus, that the quantities of lines 10-24 of claim 14 are computed, that the data is (re)combined (as in lines 28-32 of claim 14), and that the system is backwards compatible.

(1) Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes  $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ , see definition 3.3. The security of the RSA system (Section 8.2) is in fact equivalent to the integer factorization problem, see section 8.2.2(I) and Fact 8.6. It would be obvious for one of ordinary skill in the art to modify the system of

Art Unit: 2131

Section 8.2 to have a modulus having the number of primes, 'k', being a number greater than 2 because the difficulty of the integer factorization problem provides the security for the cryptosystem. Note that with this combination, we now have a cryptosystem with multiple primes, hence we no longer have just p and q but rather  $p_1, p_2, \dots, p_k$ . This is relevant in interpreting the next two paragraphs.

(2) Quisquater *et al* disclose that the quantities of lines 10-24 are computed, see page 906 first column. It would be obvious to one of ordinary skill in the art to include these computations because of Quisquater *et al*'s clear suggestion to employ the Chinese Remainder Theorem into the computations involved with the RSA cryptosystem, see the title and the abstract on page 905. Note that Quisquater *et al*'s method is described as being "fast".

(3) In the interest of producing a complete and readable action which addresses each of the claims and which utilizes the information gained by the interview (see the examiner's interview summary), the examiner here addresses two algorithms by which obviousness of recombining the data are established. The subsequent claims are each directed to one of these two algorithms. The algorithms are Gauss' Algorithm which is detailed in (a), and Garner's Algorithm, which is detailed in (b).

(a) Menezes *et al* in Section 2.4.3 discloses that the quantities of lines 28-32 are computed, see Gauss' Algorithm (Algorithm 2.121). The following are some correspondences for the reader's convenience. The applicant's  $w_i$  is Menezes *et al*'s  $N_i$ . The applicant's  $n$  is Menezes *et al*'s  $n$ . The applicant's  $Y_i$  are Menezes *et al*'s partial sums of  $x$ ,

Art Unit: 2131

where Menezes *et al* disclose that  $x$  is a sum as in Algorithm 2.121 line 2. It would be obvious to one of ordinary skill in the art to employ this algorithm for solving the Chinese Remainder Theorem (CRT) problem which arises in RSA cryptography because of Quisquater *et al*'s explicit suggestion the CRT may be used to expedite the calculation of RSA (see Quisquater *et al*'s abstract) and because Menezes *et al* discloses Gauss' Algorithm may be used to solve the CRT, see Algorithm 1.121 itself. Note that The examiner accounts for the "recursive" aspect of claim 14 by noting that computers usually compute sums as in Algorithm 2.121 recursively, and takes official notice of such. It would be obvious to compute the quantities recursively because of the added speed and memory expediency conveyed by recursive computation.

(b) Menezes *et al* in Section 14.5.2 discloses that the CRT data may be combined (or computed), see Garner's Algorithm (Algorithm 14.5.2). The following are some correspondences for the reader's convenience. Note that Garner's algorithm is recursive. It would be obvious to one of ordinary skill in the art to employ this algorithm for solving the Chinese Remainder Theorem (CRT) problem which arises in RSA cryptography because of Quisquater *et al*'s explicit suggestion the CRT may be used to expedite the calculation of RSA (see Quisquater *et al*'s abstract) and because Menezes *et al* discloses Garner's Algorithm may be used to efficiently solve the CRT, see Algorithm 1.121 itself.

(4) That the well-know RSA cryptosystem is a special case of the above combination indicates that it is backwards compatible with RSA.

Art Unit: 2131

- b. Claim 15 is similar to claim 14 except the message is decrypted using the corresponding formulae and steps. See the above.
- c. Claim 16 is a system embodiment which includes the encoding of claim 14 and the decoding of claim 15 and is rejected on analogous grounds as being obvious as such.
- d. Claims 17-21 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.
- e. Claims 22-26 are system claims for encoding and decoding a message and are therefore rejected on grounds analogous to those used to reject claims 14, 15, and 16.
- f. Claims 27-31 are method claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.
- g. Claims 32-36 are system claims for encoding a message and are therefore rejected on grounds analogous to those used to reject claim 14.
- h. Claims 37-41 are method claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 15.
- i. Claims 42-46 are system claims for decoding a message and are therefore rejected on grounds analogous to those used to reject claim 16.
- j. The examiner takes as official notice that it is notoriously well-known to those of ordinary skill in the art to use RSA type cryptography for signing and verifying messages. It would be obvious to one of ordinary skill in the art to use RSA type cryptography to sign

Art Unit: 2131

messages and verify such signatures because of the security and irrefutability available from such expedients.

i. Claims 47-51 are method claims for signing a message and are rejected on grounds analogous to those used to reject claims 14 and 15 and further in light of the above official notice.

ii. Claims 52-56 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

iii. Claims 57-61 are procedure claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

iv. Claims 62-66 are system claims for signing a message and are rejected on grounds analogous to those used to reject claims 14, 15, and 16 and further in light of the above official notice.

k. Claims 67-92 are dependent claims which are directed to two features. The examiner addresses them here.

i. Claims 67 *et al* are directed to processing the sub-tasks by way of a plurality of exponentiation units operating substantially independently. Menezes *et al* discloses simultaneous multiple exponentiation, see Note 14.87(iii) on page 617. It would be obvious to one of ordinary skill in the art to use this method in the combination recited in the parent claims

Art Unit: 2131

because of Menezes *et al*'s suggestion that efficient exponentiation is essential to employing the RSA algorithm, see the first two paragraphs of Section 14.6 Exponentiation on page 613.

ii. Claims 68 *et al* are directed to insuring that each of the random primes has the same number of bits. Menezes *et al* discloses that each of the primes used should be "roughly the same size". It would be obvious to one of ordinary skill in the art to ensure that the number of bits for each of the primes is the same because of Menezes *et al*'s suggestion that they should be roughly the same size. Note that "roughly the same size" discloses a range, which includes in the range the identity.

### ***Response to Arguments***

13. Applicant's arguments filed 18 June 2001 have been fully considered but they are not persuasive.

a. The applicant argues that the 35 USC 112 rejections of claims 14-46 regarding the limitation of the "step of decoding is accelerated" have been addressed by amendment. The examiner disagrees. Please see paragraphs 5.b and 7.a, above, for a detailed discussion.

b. The applicant traverses the 35 USC 102(b) rejections of claims 14-66 over Rivest *et al*. The thrust of the applicant's argument is that even though Rivest *et al* disclose an RSA system employing more than two primes, and even though Rivest *et al* explicitly teach of using the Chinese Remainder Theorem in conjunction therewith, Rivest *et al* do not disclose exactly how to use the Chinese Remainder Theorem in this capacity; therefore, Rivest *et al* do not

Art Unit: 2131

anticipate the claimed invention. The examiner has asserted in the prior office action that the claimed steps are inherent in using the Chinese Remainder Theorem.

i. The applicant has also argued here, as in the past, that the Chinese Remainder Theorem itself does not provide solutions, but rather merely asserts that solutions exist. More specifically, the issue is whether the Chinese Remainder Theorem provides solutions for  $k$  simultaneous modular equations. The examiner directs the applicant to paragraph 7.c of the office action of 27 April 2000 (paper 6) for a complete response. Furthermore, the examiner asserts that implementing the Chinese Remainder Theorem to solves such equations is extremely well-known to one of ordinary skill in the art. The only inventive step involves being able to see that it *can* be used in certain situations. Once it is known to use the Chinese Remainder Theorem, one of ordinary skill in the art would have no problem actually implementing it. This is evidenced by Rivest *et al* merely stating that it can be used, and not illustrating the tedious process by which it is actually implemented, presumably to avoid undue disclosure of that which is already well-known.

c. The applicant traverses the 35 USC 103 rejections of claims 67-92 over Rivest *et al* in view of Menezes *et al*. The applicant argues that Menezes *et al*'s teaching of the many benefits and methods of simultaneous multiple exponentiations in a cryptographic setting does not constitute a teaching or suggestion of employing simultaneous multiple exponentiations in hardware in a cryptographic setting. The examiner disagrees. Even assuming that Menezes *et al* do not disclose hardware implementation of the disclosed method, it is well-established in patent



Art Unit: 2131

law that it is obvious to implement software algorithms in hardware. Hence, Menezes *et al* does teach the limitation at issue.

d. The applicant traverses the 35 USC 103 rejections of claims 14-92 over Rivest *et al* in view of Quisquater. The applicant reasserts an argument that the examiner has previously addressed, namely, that Menezes *et al* does not suggest a multiple prime RSA system. The examiner directs the applicant to the examiner's response in paper 6 (the office action of 27 April 2000), paragraphs 7.b.ii and 7.b.iii.

i. The applicant further argues that neither Menezes *et al* nor Quisquater teach a specific application of the Chinese Remainder Theorem to the cryptographic arts. The examiner entirely disagrees. See Quisquater, the title and abstract of his invention. See also paragraphs 3.a and 3.b of the office action of 2 April 2001 (paper 19), where the examiner points out where Menezes *et al* discloses material refuting this argument.

e. The applicant has argued the issue of being backwards compatible.

i. The applicant argues that the 35 USC 112 rejections of claims 14-46 regarding the limitation of being "backwards compatible" have been addressed by amendment. The examiner disagrees. Please see paragraphs 5, 5.a, 5.a.i, and 5.a.ii, above, for a detailed discussion.

ii. Additionally, with regard to the 35 USC 103 rejection of claims 14-92, the applicant has questioned the examiner's assertion that, "... the well-know RSA cryptosystem is a special case of the above combination indicates that it is backwards compatible with RSA." The

Art Unit: 2131

examiner will clarify presently. The applicant's system is just the RSA cryptosystem with the possibility of having a different number of primes. Were the applicant's system to be restricted to two primes, it would not only be backwards compatible with the standard RSA system, it would *be* the standard RSA system. Hence, the backwards compatibility is obvious in this special case. Allowing backwards compatibility for a greater number of primes than two, however, presents issues that the examiner has addressed by way of 35 USC 112 rejections. Please see paragraphs 5, 5.a, 5.a.i, and 5.a.ii, above.

### *Conclusion*

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Rivest *et al* (US 4,405,829, see column 13 lines 29-34) and Slavin (US 5,974,151, see the abstract) disclose multi-prime (more than two) RSA systems.

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

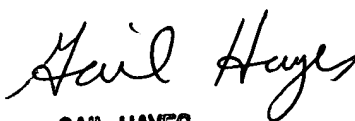
16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey Scott Leaning whose telephone number is (703) 306-5975. The examiner can normally be reached on weekdays from 9:00am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned is (703) 308-9051.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jeffrey Scott Leaning

2 August 2001



**GAIL HAYES**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2100**